PATENT ABSTRACTS OF JAPAN

(11)Publication number : 06-069962
(43)Date of publication of application : 11.03.1994

(51)Int.Cl. H04L 12/66
H04L 9/00
H04L 9/10
H04L 9/12
H04L 12/28
H04L 12/56

(21)Application number : 04-240046
(22)Date of filing : 17.08.1992

(71)Applicant : FUJI XEROX CO LTD
(72)Inventor : OTA HIROMI

(54) NETWORK CONNECTOR AND NETWORK COMMUNICATION SYSTEM

(57)Abstract:
PURPOSE: To conceal between which terminators communication is implemented and to conceal the content of the communication by sending data subjected to capsule processing while composing the data into a packet.
CONSTITUTION: A ciphering decision section 42 checks whether or not a path selected by a path selection section 11 is equivalent to a path stored in a secrecy protection required path storage section 43 and decides ciphering of packet data when the path is equivalent to the secrecy protection required path. The ciphering is implemented by a ciphering/decoding processing section 40. Then a data capsule processing section 41 implements processing of incorporating ciphered data into a packet as transmission data by selecting a network connector located in a region at the outside of secrecy protection range as if it were a final destination and using its own network connector as if it were a first sender. In this casewhen it is clear that the data are ciphered datathe ciphering/decoding processing section 40 decodes the data into the original packet and the decoded data are sent to a final equipment being

a true final destination.

<hr size=2 width="100%" align=center>

CLAIMS

[Claim(s)]

[Claim 1]It is provided in a part which connects two or more subnetworks since a network which communicates by a connectionless type packet is constitutedIn a network connection apparatus which analyzes information on a received packetselects a sending-out courseand sends out a new packetA security required path storage section which makes a range which cannot carry out security memorize for every sending-out courseAn encryption deciding part which opts for a data encryption about a network layer of a packet when it is what passes a security required course in which transfer paths selected based on a final destination of a packet are remembered to be encryption and a decoding processing part by said security required path storage sectionA network connection apparatus which is provided with an encapsulation part which processes a network connection apparatus located in a place which escaped from a range which cannot carry out security as a final destination of said enciphered dataand is characterized by building encapsulated data into a packet and sending it out.

[Claim 2]In a network communication system in a network which two or more subnetworks which communicate using a connectionless type packet are connected via a network connection apparatusand changesWhen a range which cannot carry out security is included in a course to a final destination of a received packet in a network connection apparatus of the transmitting sideEncipher data about a network layer of a received packetand build a network connection apparatus in a part beyond said range into a packet new as a final destination of said enciphered dataand it is sent outA network communication system decrypting enciphered data in a network connection apparatus made into a final destinationand sending out to the next.

DETAILED DESCRIPTION

[Detailed Description of the Invention]

[0001]

[Industrial Application]This invention relates to the network connection apparatus and network communication system in the network which comprises two or more subnetworks which communicate using a connectionless type packet.

[0002]

[Description of the Prior Art]Packet communication includes connection-oriented type (or connection oriented type) packet communication and connectionless type

packet communication. Connection-oriented type packet communication performs transmission (phase 3) of information or a message main partafter performing connection (phase 1) of a communication lineand setting out and establishment (phase 2) of a data link. Connectionless type packet communication performs the phase 3 suddenly. This invention is related to the latter.

[0003]There are some which two or more subnetworks were connected via the network connection apparatusand were constituted in the network of data communications. Howeverif it communicated in the form as it isthere are some which cannot keep secrecy in a subnetwork.

[0004]Secrecy cannot be kept in a subnetwork connectable by the 3rd unspecified personsuch as ordinary public circuit exchange network and a public telephone network. Such a subnetwork is called Black subnetwork. On the other handthe subnetwork in which connection by the 3rd unspecified person is impossible is called White subnetwork like the line switching network in a companyor LAN in a company (Local Area Network).

[0005]Drawing 6 is a figure showing one example of the network with which the subnetwork of Black and the subnetwork of White are contained. In drawing 6a terminating setE-Hand K of 50-56 are subnetworks a network connection apparatusand 57-59. It is an end user of data communicationsand a packet is first sent from these and the terminating sets 57-59 are eventually sent into these. The network connection apparatus 50-56 make connection between subnetworks. In this examplethe subnetwork H is Black and the subnetwork K is White.

[0006]When sending a packet to the terminating set 59 from the terminating set 57the following two courses can be considered. The 1st course is a course of the terminating-set 57 -> network connection apparatus 52 -> subnetwork K-> network connection apparatus 56 -> terminating set 59. The 2nd course is a course of the terminating-set 57 -> network connection apparatus 51 -> subnetwork H-> network connection apparatus 55 -> terminating set 59. Since it passes along the subnetwork H of Black when sent in the 2nd coursesecurity is not guaranteed.

[0007]Thenthe applicant has already proposed the network communication system sent after checking a partner by exchanging passwords a priori as a communication method for security (Japanese Patent Application No. No. 26900 [four to]). Drawing 2 is a figure showing the network connection apparatus used with such a communication method. in drawing 2 -- 10 -- a destination deciding part and 11 -- a channel selection part and 12 -- a path storage section and 14 are [a reliability determination part and R of an interface and 16] network connection apparatus a certification information reply part and 17 a packet treating part and 15 the course Management Department and 13.

[0008]each interface 15 -- LANa public networkand a dedicated line -- it is an interface for connecting.

The internal configuration changes with partners who connect.

It is provided suitably to what kind of subnetwork these interfaces are connected.
[0009]The packet received via a certain interface is sent out via another interfaceafter being processed by the packet treating part 14. The packet treating part 14 reads the information on the received packetand processes it in the form which can be sent out to the next destination (for examplethe following address is given). When the destination deciding part 10 – the path storage section 13 carry out the processingthey play an auxiliary role.
[0010]The path storage section 13 has memorized the database about a network courseand when there are deletion of a coursechangean additionetc.the course Management Department 12 updates a database and manages it. The channel selection part 11 refers to the data of the path storage section 13and chooses the course which sends a packet. The destination deciding part 10 determines the part which should be transmitted to the next.
[0011]The reliability determination part 17 determines whether the selected course can trust it on security. The password first provided in the partner's network connection apparatus which it is trying to send beforehand is sent. It is judged as the partner who can trust it if certification information is replied from a partnerand data is sent. The certification information reply part 16 is a portion which replies certification informationwhen self receives a password.
[0012]As document about the conventional technology of such data communicationsthey are JP64-68044A and the publication number 3for example. – There is a No. 13146 gazette.
[0013]
[Problem(s) to be Solved by the Invention](Problem) Howeverin the communication directly performed by Hazama of network connection apparatus who has defined the password of security beforehandin the network connection apparatus and network communication system of the above mentioned former which perform security by password exchangecan carry out securitybut. Among the middles were other network connection apparatusandin the communication indirectly performed via itthere was a problem that security could not be carried out.
[0014](Explanation of a problem) In drawing 6the network connection apparatus 51 and the network connection apparatus 55 presuppose that it is a network connection apparatus like drawing 2 constituted so that password exchange for security could be performed. When both up a circuita course judges Black or White.
[0015]Howeverwhen a course consists of two or more subnetworks and other network connection apparatus intervene in betweensecurity may not be able to be carried out in password exchange. Nextthe example is shown.
[0016]Drawing 10 is other examples of the network which comprises two or more subnetworks. As for A–Da terminating setand 7–9 are network connection apparatus a subnetworkand 1–6. The subnetwork ACand D is LAN (Local Area Network)for exampleand the subnetwork B is a public network (X.25).

[0017]The terminating set which is an end user is connected to each subnetwork. For examplethe terminating sets 1 and 2 are connected to the subnetwork A. Connection between a subnetwork and a subnetwork is made by a network connection apparatus. For exampleconnection between the subnetwork A and the subnetwork B is made by the network connection apparatus 7.
[0018]To the terminating set and network connection apparatus in a networkthe network address accepted in the whole network and the subnetwork address accepted within the subnetwork which is involving are given. Since the number of the subnetworks in which a terminating set participates is onethe number of the subnetwork addresses is onebut since the subnetwork in which a network connection apparatus participates is pluralitytwo or more subnetwork addresses are given.
[0019]A packet is first sent out from a certain terminating setand attains the purpose by being sent to other terminating sets. When sending to the terminating set of other subnetworksit is sent via a network connection apparatus. For examplewhen sending to the terminating set 6 from the terminating set 1 of drawing 10as a dotted line showsit is sent in the course of the terminating-set 1 -> network connection apparatus 7 -> network connection apparatus 8 -> network connection apparatus 9 -> terminating set 6.
[0020]Since the subnetwork B is a public networkwhen it passes along thissecrecy may leakand there is doubt of Black. Temporarilyeven if the network connection apparatus 7 and 8 can perform communication which carried out security by password exchangesecrecy may leak in the network which intervenes on the wayand they cannot necessarily perform secret protection thoroughly.
[0021]Becausein the subnetwork which the packet transmitted passes on the waythe information about a data contenta final destinationetc. may be stolen by a certain means.
[0022]In the network containing LAN which was described above. As the protocol systemThe basic reference model of open systems interconnection as shown in drawing 8 (Open Systems Interconnection Basic ISO 7498 Information processing systems) referencemodel is adopted. This comprises seven layersthe 1st layer physical layerthe 2nd layer data link layerthe 3rd layer network layerthe 4th layer transport layerthe 5th layer session layerthe 6th layer presentation layerand the 7th layer application layer. Thereforecomposition of a packet is also made into the form where this protocol system was followed.
[0023]Drawing 7 is a figure showing the composition of a packet. 20 a packet and 21 an address subnetwork address and 22 A transmitting subnetwork addressAs for 23 and 25a data division and 24D other information bureaus and 24 Packet dataAs for a final destination device network address and 2826 is [other information bureaus and 30] data of the 4-7th layer a transmission source device network address and 29 a protocol header and Fixed Partand 27. The packet data 24D are stored in the data division 24.

[0024]The packet at the time of shipping towards the terminating set 6 from the terminating set 1 of the network of drawing 10 is taken for an exampleand the value indicated to each address of address subnetwork address 21 grade is explained. A subnetwork address will attach and express the numerals (ABCD) of a related subnetworkand a network address will attach and express N. In the transmitting subnetwork address 22the address of the part which sends out this packeti.e.the subnetwork address of the terminating set 1(1A) is indicated.
[0025]In the address subnetwork address 21if the terminating set 6 is in the same subnetwork A as the terminating set 1the subnetwork address of the terminating set 6 will be indicated. Howeversince the terminating set 6 is in Haruka or the left subnetwork Din order to go thereit must go exceeding other subnetworks. In such a casethe subnetwork address (7A) about the subnetwork A of the network connection apparatus 7 which is the present address is indicated. Thusthe address subnetwork address 21 and the transmitting subnetwork address 22 are rewritten whenever it exceeds a subnetwork.
[0026]The network address (6N) of the terminating set 6 to send into the final destination device network address 27 eventually is indicatedand the network address (1N) of the transmitting agency terminating set 1 sent out first is indicated at the transmission source device network address 28. After each packet reaches the terminating set 6 which is a final destinationit is assembled by the order specified at the time of sending out.
[0027]Drawing 9 is a figure showing change of the composition of the packet which has a network of drawing 10 conveyed. Numerals support the thing of drawing 7. From the terminating set 1drawing 9 (b) is the packet composition in the case of sending to the network connection apparatus 7and was already described.
[0028]Drawing 9 (**) is the packet composition in the case of sending to the network connection apparatus 8 from the network connection apparatus 7. The transmitting subnetwork address 22 is rewritten with the subnetwork address (7B) about the subnetwork B of the network connection apparatus 7The address subnetwork address 21 is rewritten by the subnetwork address (8B) about the subnetwork B of the network connection apparatus 8. The transmission source device network address 28 and the final destination device network address 27 remain the same.
[0029]Drawing 9 (**) is the packet composition in the case of sending to the network connection apparatus 9 from the network connection apparatus 8. The transmitting subnetwork address 22 is rewritten with the subnetwork address (8C) about the subnetwork C of the network connection apparatus 8The address subnetwork address 21 is rewritten by the subnetwork address (9C) about the subnetwork C of the network connection apparatus 9. The transmission source device network address 28 and the final destination device network address 27 remain the same.
[0030]Drawing 9 (**) is the packet composition in the case of sending to the terminating set 6 from the network connection apparatus 9. The transmitting

subnetwork address 22 is rewritten with the subnetwork address (9D) about the subnetwork D of the network connection apparatus 9and the address subnetwork address 21 is rewritten by the subnetwork address (6D) of the terminating set 6. The transmission source device network address 28 and the final destination device network address 27 remain the same.

[0031]Thusa packet is an intermediate subnetwork and network connection apparatusand since it is analyzed the communication to which terminating set from which terminating set it isin going via a subnetwork and a network connection apparatus without the guarantee of securitythere is a possibility that data may be stolen. This invention makes it SUBJECT to solve such a problem.

[0032]

[Means for Solving the Problem]It is provided in a part which connects two or more subnetworks since a network which communicates by a connectionless type packet in this invention in order to solve said SUBJECT is constitutedIn a network connection apparatus which analyzes information on a received packetselects a sending-out courseand sends out a new packetA security required path storage section which makes a range which cannot carry out security memorize for every sending-out courseAn encryption deciding part which opts for a data encryption about a network layer of a packet when it is what passes a security required course in which transfer paths selected based on a final destination of a packet are remembered to be encryption and a decoding processing part by said security required path storage sectionWe had an encapsulation part which processes a network connection apparatus located in a place which escaped from a range which cannot carry out security as a final destination of said enciphered dataand decided to build encapsulated data into a packet and to send it out.

[0033]In a network communication system in a network which two or more subnetworks which communicate using a connectionless type packet are connected via a network connection apparatusand changesWhen a range which cannot carry out security is included in a course to a final destination of a received packet in a network connection apparatus of the transmitting sideEncipher data about a network layer of a received packetand build a network connection apparatus in a part beyond said range into a packet new as a final destination of said enciphered dataand it is sent outIn a network connection apparatus made into a final destinationwe decided to decrypt enciphered data and to send out to the next.

[0034]

[work --] for In a network which two or more subnetworks which communicate using a connectionless type packet are connected via a network connection apparatus in this inventionand changesWhen it is going to carry out secret communication between points which sandwiched a subnetwork which cannot carry out securitya network connection apparatus which had special composition in those points is installed.

[0035]When a range which cannot carry out security is in a course which transmits

from there in this network connection apparatusData including address information of the first transmitting terminating set and the last address terminating set is encipheredand it has packet composition addressed to a network connection apparatus located in a place which escaped from a range which cannot carry out security of itand sends (encapsulation). A network connection apparatus which received it decrypts enciphered dataand sends it to a terminating set of a final destination with the usual packet composition.

[0036]If it is within limits which cannot carry out securitysince it passes in a form of the usual packet addressed to a network connection apparatus located in a place which escaped from the rangethe fact among which terminating sets communication was really performed can be hidden. Since it is enciphereddata can hide the contents.

[0037]

[Example]Hereafterworking example of this invention is described in detail based on Drawings. Drawing 1 is a network connection apparatus of this invention. Numerals correspond to the thing of drawing 2 andas for encryption and a decoding processing partand 41an encryption deciding part and 43 are security required path storage sections a data encapsulation part and 42 40. These are the composition provided specially because of security. The network connection apparatus which has such composition is installed in the connection section of the subnetwork which can carry out securityand the subnetwork which is not made. Hereaftereach formation part is explained. Since the thing of the same numerals as drawing 2 achieves the same operation and a functionthe explanation is omitted.

[0038]The security required path storage section 43 memorizes whether security is guaranteed to which network connection apparatuswhen sending a packet in which course. For examplethe security required path storage section 43 of the network connection apparatus 7 of drawing 10 remembers the network connection apparatus 9 that security is not guaranteedwhen sending out in the direction of the subnetwork B.

[0039]The encryption deciding part 42 investigates whether the course selected in the channel selection part 11 is equivalent to the course memorized to the security required path storage section 43and when it correspondsit determines to encipher the packet data 24D of drawing 7. Encryption is performed by encryption and the decoding processing part 40. Arbitrary things can be used for the technique of encryption. Encryption and the decoding processing part 40 also perform decryptingwhen the enciphered data is received.

[0040]The data encapsulation part 41 makes a final destination the network connection apparatus located in the place which escaped from the range which cannot carry out securityand a self network connection apparatus as first transmitting originProcessing incorporated in a packet by using the aforementioned encryption data as send data (this is made [of explanation] "encapsulation" for convenience) is carried out.

[0041]Drawing 3 is a figure showing the composition of the packet which encapsulated

encryption data. Numerals correspond to the thing of drawing 7 and a capsule construct and 32 31 A protocol and FixedPartAs for a final destination network connection apparatus network address and 34other information bureaus and 36 are encryption data storing parts a transmitting agency network connection apparatus network address and 35 33.

[0042]When it becomes clear that it must send out to the course which cannot do security as a result of analyzing the received packet with the network connection apparatus of this inventionThe packet data 24D about a network layer are encipheredand it is stored in the encryption data storing part 36 as the same treatment as the send data of the usual packet.

[0043]At and equivalent to the final destination device network address 27 (refer to drawing 7) in the usual packet compositionthen the final destination network connection apparatus network address 33 at the time. The network address of the network connection apparatus located in the place which escaped from the range which cannot carry out security is indicated. At equivalent to the transmission source device network address 28 (refer to drawing 7) in the usual packet compositionthen the transmitting agency network connection apparatus network address 34 at the time. The network address of the network connection apparatus which is going to shipself network addressi.e.packetis indicated.

[0044]Drawing 4 shows the example of the packet which stored encapsulation data. Since this is a network of drawing 10 and it is a range which cannot carry out security between the network connection apparatus 7 and 9In order to carry out communication from which secrecy does not leak among bothin the environment where the network connection apparatus of this invention is used as the network connection apparatus 7 and 9the packet sent to the terminating set 6 from the terminating set 1 is a thing in the state where it was remade with the network connection apparatus 7.

[0045]Numerals support the thing of drawing 3. The address of the transmission source device network address 28 is made into the network address (1N) of the terminating set 1It is enciphered in a form as it isand the packet data 24D in which the final destination device network address 27 was made into the network address (6N) of the terminating set 6 are stored in the encryption data storing part 36. Let the transmitting agency network connection apparatus network address 34 be a network address (7N) of the network connection apparatus 7 which is just going to ship this packet now. Let the final destination network connection apparatus network address 33 be a network address (9N) of the network connection apparatus 9 located in the place which escaped from the range which cannot carry out security.

[0046]The network connection apparatus 7 with which the transmitting subnetwork address 22 is just going to ship this packet nowIt is considered as the subnetwork address (7B) about the subnetwork Band let the address subnetwork address 21 be a subnetwork address (8B) about the subnetwork B of the network connection

apparatus 8 which is the present destination.
[0047]If a packet is sent with such compositionin the intermediate network connection apparatus which cannot carry out securityit will be dealt with as a usual packet whose first transmitting origin is the network connection apparatus 7 and whose final address is the network connection apparatus 9. Thereforethe network connection apparatus located in the place which escaped from the range which cannot carry out security is sent not understood at alland where true transmitting origin and a true final destination are goes. Even if it tries to steal send data with an intermediate network connection apparatussince it is encipheredthe portion cannot know the contents.
[0048]Although the network connection apparatus 9 located in the place which escaped from the range which cannot carry out security is also used as the network connection apparatus which has the composition of this inventionif a packet is receivedit will be judged whether it is what has been enciphered and encapsulated. The judgment is made by investigating whether it has passed along the course registered into the security required path storage section 43 as where a transmitting agency is (in the case of an upper example network connection apparatus 7).
[0049]When it becomes clear that it is encipheredit decrypts to the original packet data 24D by encryption and the decoding processing part 40and this is sent to the terminating set 6 which is a true final destination with the usual packet composition.
[0050]Drawing 5 is a flow chart showing a send action which the network connection apparatus of this invention mentioned above.
Step 1 -- A packet is received.
Step 2 -- The received packet is analyzeda course is chosen and the address which transmits to the next is determined.
Step 3 -- That the selected course takes the measure of security checks with reference to the security required path storage section 43 for whether it is a required course. If it does not passit transmits to the nextwithout taking the measure of security.
Step 4 -- When it passes along the course which needs securitysend data is enciphered including the information on the final destination and first transmitting origin.
Step 5 -- The enciphered data is encapsulated.
Step 6 -- It transmits to the following address.
[0051]In order to carry out the network communication system of this inventionIt is not necessary to change the network connection apparatus of the whole network into the thing of the composition of this inventionand since what is necessary is to install the network connection apparatus of this invention only in the point which is going to carry out communication which only carried out securityit can carry out easily at cheap cost.
[0052]

[Effect of the Invention]As stated aboveaccording to the network connection apparatus and network communication system of this invention. When the range which cannot carry out security is in the course which transmits from there when it is going to carry out secret communication between the points which sandwiched the subnetwork which cannot carry out securityData including the first transmitting terminating set and the last address terminating set is encipheredand it has packet composition addressed to a network connection apparatus located in the place which escaped from the range which cannot carry out security of itand sends (encapsulating).

[0053]Thereforeif it is within limits which cannot carry out securitysince it passes in the form of the usual packet addressed to a network connection apparatus located in the place which escaped from the rangethe fact among which terminating sets communication was really performed can be hidden. Since it is enciphereddata can hide the contents.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1]A network connection apparatus of this invention

[Drawing 2]The conventional network connection apparatus

[Drawing 3]The figure showing the general composition of the packet which stored encapsulation data

[Drawing 4]The figure showing the example of the packet which stored encapsulation data

[Drawing 5]The flow chart showing the send action of the network connection apparatus of this invention

[Drawing 6]The figure showing one example of the network with which the subnetwork of Black and the subnetwork of White are contained

[Drawing 7]The figure showing the composition of a packet

[Drawing 8]The figure showing the basic reference model of open systems interconnection

[Drawing 9]The figure showing change of the composition of the packet which has a network of drawing 10 conveyed

[Drawing 10]The figure showing other examples of the network which comprises two or more subnetworks

[Description of Notations]

1-6 — A terminating set7-9 — A network connection apparatus10 — Destination deciding part11 [— Packet Management Department] — A channel selection part12 — The course Management Department13 — A path storage section14 15 — An interface16 — A certification information reply part17 — Reliability determination

part20 — A packet24D24D$_1$24D$_2$ — Packet data31 [— An encryption deciding part43 / — A security required path storage section50-56 / — A network connection apparatus57-59 / — A terminating setA-HK / — A subnetwork and R are network connection apparatus.] — A capsule construct40 — Encryption and a decoding processing part41 — A data encapsulation part42

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号

特開平6－69962

(43)公開日　平成６年(1994)３月11日

(51)Int.Cl.[5]	識別記号	庁内整理番号	ＦＩ		技術表示箇所
Ｈ０４Ｌ 12/66					
9/00					
9/10					
		8529－5Ｋ	Ｈ０４Ｌ 11/20	Ｂ	
		7117－5Ｋ	9/00	Ｚ	

審査請求　未請求　請求項の数２(全　９　頁)　最終頁に続く

(21)出願番号　特願平4－240046

(22)出願日　平成４年(1992)８月17日

(71)出願人　000005496
富士ゼロックス株式会社
東京都港区赤坂三丁目３番５号

(72)発明者　太田　裕美
神奈川県川崎市高津区坂戸３丁目２番１号
ＫＳＰＲ&Ｄ　ビジネスパークビル　富士ゼロックス株式会社

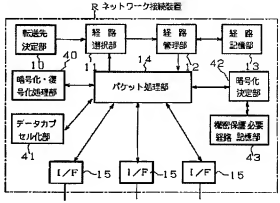
(74)代理人　弁理士　本庄　富雄　（外１名）

(54)【発明の名称】　ネットワーク接続装置およびネットワーク通信方式

(57)【要約】

【目的】　コネクションレス型パケットを用いて通信する複数のサブネットワークから成るネットワークにおけるネットワーク接続装置およびネットワーク通信方式において、機密保護を行うこと。

【構成】　機密保護し得ないサブネットワークを挟んだ地点間で機密の通信をしようとする場合に、それらの地点に、図のような特別の構成を持ったネットワーク接続装置Ｒを設置する。このネットワーク接続装置では、そこから送信する経路中に機密保護し得ない範囲がある場合には、最初の送信終端装置および最後の宛先終端装置を含めてデータを暗号化し、それを機密保護し得ない範囲を抜けたところに位置するネットワーク接続装置宛のパケット構成にして送る。それを受け取ったネットワーク接続装置は、暗号化されたデータを復号化し、最終宛先の終端装置へ、通常のパケット構成で送る。



【特許請求の範囲】

【請求項1】　コネクションレス型パケットにより通信を行うネットワークを構成するため複数のサブネットワークを接続する個所に設けられ、受け取ったパケットの情報を解析して送出経路を選定し新たなパケットを送出するネットワーク接続装置において、機密保護し得ない範囲を送出経路毎に記憶させておく機密保護必要経路記憶部と、暗号化および復号化処理部と、パケットの最終宛先に基づいて選定した転送経路が前記機密保護必要経路記憶部に記憶されている機密保護必要経路を通過するものである場合にパケットのネットワーク層に関するデータの暗号化を決定する暗号化決定部と、機密保護し得ない範囲を抜けたところに位置するネットワーク接続装置を前記暗号化したデータの最終宛先として処理するカプセル化部とを具え、カプセル化したデータをパケットに組み込んで送出することを特徴とするネットワーク接続装置。

【請求項2】　コネクションレス型パケットを用いて通信する複数のサブネットワークがネットワーク接続装置を介して接続されて成るネットワークにおけるネットワーク通信方式において、送信側のネットワーク接続装置では、受け取ったパケットの最終宛先までの経路中に機密保護し得ない範囲が含まれている場合に、受け取ったパケットのネットワーク層に関するデータを暗号化し、前記範囲を越えた個所にあるネットワーク接続装置を前記暗号化したデータの最終宛先として新たなパケットに組み込んで送出し、最終宛先とされたネットワーク接続装置では、暗号化されたデータを復号化して次へ送出することを特徴とするネットワーク通信方式。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明は、コネクションレス型パケットを用いて通信する複数のサブネットワークから成るネットワークにおけるネットワーク接続装置およびネットワーク通信方式に関するものである。

【０００２】

【従来の技術】パケット通信には、コネクションオリエンテッド型（またはコネクション型）パケット通信と、コネクションレス型パケット通信とがある。コネクションオリエンテッド型パケット通信は、通信回線の接続（フェーズ１），データリンクの設定と確立（フェーズ２）を行ってから、情報あるいはメッセージ本体の伝送（フェーズ３）を行うものである。コネクションレス型パケット通信は、いきなりフェーズ３を行うものである。本発明は、後者に関係している。

【０００３】データ通信のネットワークには、複数のサブネットワークがネットワーク接続装置を介して接続されて構成されたものがある。しかしながら、サブネットワークには、そのままの形で通信したのでは、機密の守れないものがある。

【０００４】一般公衆回線交換網や公衆電話網などの不特定の第３者によって接続可能なサブネットワークでは、機密を守ることができない。このようなサブネットワークは、Ｂlack なサブネットワークと言われる。一方、企業内回線交換網や企業内ＬＡＮ（Local Area Network）のように、不特定の第３者による接続が不可能なサブネットワークは、White なサブネットワークと言われる。

【０００５】図６は、Ｂlack のサブネットワークとＷhite のサブネットワークとが含まれているネットワークの１例を示す図である。図６において、５０～５６はネットワーク接続装置、５７～５９は終端装置、Ｅ～Ｈ，Ｋはサブネットワークである。終端装置５７～５９が、データ通信のエンドユーザーであり、最初にこれらからパケットは発信され、最終的にこれらに送り届けられる。ネットワーク接続装置５０～５６は、サブネットワーク間の接続を行う。この例では、サブネットワークＨはＢlack であり、サブネットワークＫはＷhite である。

【０００６】終端装置５７から終端装置５９へパケットを送る場合、次の２つの経路が考えられる。第１の経路は、終端装置５７→ネットワーク接続装置５２→サブネットワークＫ→ネットワーク接続装置５６→終端装置５９という経路である。第２の経路は、終端装置５７→ネットワーク接続装置５１→サブネットワークＨ→ネットワーク接続装置５５→終端装置５９という経路である。第２の経路で送られた場合、Ｂlack のサブネットワークＨを通るので、機密保護は保証されない。

【０００７】そこで、機密保護のための通信方式として、事前にパスワードを交換することにより、相手を確認してから送るネットワーク通信方式を、出願人は既に提案している（特願平４－　26900号）。図２は、そのような通信方式で用いられるネットワーク接続装置を示す図である。図２において、１０は転送先決定部、１１は経路選択部、１２は経路管理部、１３は経路記憶部、１４はパケット処理部、１５はインタフェース、１６は認証情報返信部、１７は信頼性決定部、Ｒはネットワーク接続装置である。

【０００８】各インタフェース１５は、例えばＬＡＮとか公衆回線網とか専用線とかと接続するためのインタフェースであり、接続する相手によってその内部構成は異なる。これらのインタフェースは、どのようなサブネットワークに接続するかによって、適宜設けられる。

【０００９】或るインタフェースを介して受け取られたパケットは、パケット処理部１４で処理された後、別のインタフェースを介して送り出される。パケット処理部１４は、受け取ったパケットの情報を読み取り、次の転送先へ送り出せる形に処理する（例えば、次の宛先を付与する）。転送先決定部１０～経路記憶部１３は、その処理をする際に補助的な役割を果たす。

【００１０】経路記憶部１３はネットワークの経路に関

するデータベースを記憶しており、経路管理部１２は、経路の削除，変更，追加等があった場合にデータベースを更新して管理する。経路選択部１１は、経路記憶部１３のデータを参考にして、パケットを送る経路を選択する。転送先決定部１０は、次に転送すべき箇所を決定する。

【００１１】信頼性決定部１７は、選択した経路が機密保護の上で信頼できるか否か決定する。送ろうとしている相手のネットワーク接続装置に、まず予め定めてあるパスワードを送ってみる。相手から認証情報が返信されて来ると信頼できる相手と判断し、データを送る。認証情報返信部１６は、自己がパスワードを受け取った場合に、認証情報を返信する部分である。

【００１２】このようなデータ通信の従来技術に関する文献としては、例えば特開昭64－68044 号公報，特開平３－ 13146号公報がある。

【００１３】

【発明が解決しようとする課題】（問題点）しかしながら、パスワード交換によって機密保護を行う前記した従来のネットワーク接続装置およびネットワーク通信方式では、予め機密保護のパスワードを定めているネットワーク接続装置同士の間で直接行う通信の場合には機密保護できるが、途中に他のネットワーク接続装置等があり、それを介して間接的に行う通信の場合には機密保護できないという問題点があった。

【００１４】（問題点の説明）図６において、ネットワーク接続装置５１とネットワーク接続装置５５とが、機密保護のためのパスワード交換を行い得るよう構成された、図２のようなネットワーク接続装置であるとする。両者は回線をupする際、経路がBlack かWhiteかを判断する。

【００１５】しかし、経路が複数のサブネットワークからなり、間に他のネットワーク接続装置が介在するような場合は、パスワード交換では機密保護できない場合がある。次に、その例を示す。

【００１６】図１０は、複数のサブネットワークから成るネットワークの他の例である。A～Dはサブネットワーク，１～６は終端装置、７～９はネットワーク接続装置である。サブネットワークA，C，Dは、例えばＬＡＮ（Local Area Network）であり、サブネットワークＢは、公衆回線網（Ｘ．２５）である。

【００１７】各サブネットワークには、エンドユーザーである終端装置が接続されている。例えば，サブネットワークAには、終端装置１，２が接続されている。サブネットワークとサブネットワークとの接続は、ネットワーク接続装置によって行われる。例えば，サブネットワークAとサブネットワークＢとの接続は、ネットワーク接続装置７によって行われる。

【００１８】ネットワーク内にある終端装置やネットワーク接続装置に対しては、ネットワーク全体で通用するネットワークアドレスと、閉ちているサブネットワーク内で通用するサブネットワークアドレスとが付与されている。終端装置が関与するサブネットワークは１つであるから、そのサブネットワークアドレスは１つであるが、ネットワーク接続装置が関与するサブネットワークは複数であるから、複数個のサブネットワークアドレスが付与されている。

【００１９】パケットは、最初に或る終端装置から送り出され、他の終端装置へ届けられることにより、目的を達する。他のサブネットワークの終端装置へ送る場合には、ネットワーク接続装置を経由して届けられる。例えば、図１０の終端装置１から終端装置６へ送る場合には、点線で示すように、終端装置１→ネットワーク接続装置７→ネットワーク接続装置８→ネットワーク接続装置９→終端装置６という経路で届けられる。

【００２０】サブネットワークＢは公衆回線網であるため、ここを通るときに機密が漏れる可能性があり、Black の疑いがある。仮に、ネットワーク接続装置７，８はパスワード交換により機密保護をした通信が出来るものであったとしても、途中に介在するネットワークで機密が漏れる場合もあり、完全に機密の保護ができるわけではない。

【００２１】なぜなら、転送されるパケットは、途中で通過するサブネットワークにおいて、何らかの手段によってデータ内容や最終宛先等に関する情報が盗まれる可能性がある。

【００２２】前記したようなＬＡＮを含むネットワークでは、そのプロトコル体系として、図８に示すような開放型システム間相互接続の基本参照モデル（ISO 7498 Information processing systems, Open Systems Interconnection Basic referencemodel ）が採用されている。これは，第１層物理層，第２層データリンク層，第３層ネットワーク層，第４層トランスポート層，第５層セッション層，第６層プレゼンテーション層，第７層アプリケーション層の７層から構成されている。従って、パケットの構成も、このプロトコル体系に則った形になされる。

【００２３】図７は、パケットの構成を示す図である。２０はパケット、２１は宛先サブネットワークアドレス、２２は送信サブネットワークアドレス、２３，２５はその他の情報部、２４はデータ部、２４Ｄはパケットデータ、２６はプロトコルヘッダおよびFixed Part、２７は最終宛先装置ネットワークアドレス、２８は送信元装置ネットワークアドレス、２９はその他の情報部、３０は第４～７層のデータである。データ部２４には、パケットデータ２４Ｄが格納される。

【００２４】図１０のネットワークの終端装置１から終端装置６に向けて発送する際のパケットを例にとり、宛先サブネットワークアドレス２１等の各アドレスに記載する値について説明する。なお、サブネットワークアド

レスは、関係するサブネットワークの符号（A，B，C，D）を付して表し、ネットワークアドレスはNを付して表すことにする。送信サブネットワークアドレス22には、このパケットを送りだす箇所のアドレス、つまり終端装置1のサブネットワークアドレス（1A）を記載する。

【0025】宛先サブネットワークアドレス21には、もし、終端装置6が終端装置1と同じサブネットワークA内にあれば、終端装置6のサブネットワークアドレスが記載される。しかし、終端装置6は遙か離れたサブネットワークDにあるので、そこへ行くためには、他のサブネットワークを越えて行かなければならない。そういう場合には、当面の宛先であるネットワーク接続装置7の、サブネットワークAに関するサブネットワークアドレス（7A）が記載される。このように、宛先サブネットワークアドレス21と送信サブネットワークアドレス22とは、サブネットワークを越える毎に、書き換えられる。

【0026】最終宛先装置ネットワークアドレス27には、最終的に送り届けたい終端装置6のネットワークアドレス（6N）が記載され、送信元装置ネットワークアドレス28には、最初に送り出す送信元終端装置1のネットワークアドレス（1N）が記載される。各パケットは最終宛先である終端装置6に到着した後、送出時に指定した順序に組み立てられる。

【0027】図9は、図10のネットワークを搬送されるパケットの構成の変化を示す図である。符号は図7のものに対応している。図9（イ）は、終端装置1からネットワーク接続装置7へ送る場合のパケット構成であり、既に述べた。

【0028】図9（ロ）は、ネットワーク接続装置7からネットワーク接続装置8へ送る場合のパケット構成である。送信サブネットワークアドレス22が、ネットワーク接続装置7のサブネットワークBに関するサブネットワークアドレス（7B）と書き換えられ、宛先サブネットワークアドレス21が、ネットワーク接続装置8のサブネットワークBに関するサブネットワークアドレス（8B）に書き換えられている。送信元装置ネットワークアドレス28，最終宛先装置ネットワークアドレス27は、元のままである。

【0029】図9（ハ）は、ネットワーク接続装置8からネットワーク接続装置9へ送る場合のパケット構成である。送信サブネットワークアドレス22が、ネットワーク接続装置8のサブネットワークCに関するサブネットワークアドレス（8C）と書き換えられ、宛先サブネットワークアドレス21が、ネットワーク接続装置9のサブネットワークCに関するサブネットワークアドレス（9C）に書き換えられている。送信元装置ネットワークアドレス28，最終宛先装置ネットワークアドレス27は、元のままである。

【0030】図9（ニ）は、ネットワーク接続装置9から終端装置6へ送る場合のパケット構成である。送信サブネットワークアドレス22が、ネットワーク接続装置9のサブネットワークDに関するサブネットワークアドレス（9D）と書き換えられ、宛先サブネットワークアドレス21が終端装置6のサブネットワークアドレス（6D）に書き換えられている。送信元装置ネットワークアドレス28，最終宛先装置ネットワークアドレス27は、元のままである。

【0031】このように、パケットは、途中のサブネットワークやネットワーク接続装置で、どの終端装置からどの終端装置への通信経路を選定か等が解析されるから、機密保護の保証がないサブネットワークやネットワーク接続装置を経由する場合には、データが盗まれる恐れがある。本発明は、このような問題点を解決することを課題とするものである。

【0032】

【課題を解決するための手段】前記課題を解決するため、本発明では、コネクションレス型パケットにより通信を行うネットワークを構成するため複数のサブネットワークを接続する個所に設けられ、受け取ったパケットの情報を解析して送出経路を選定し新たなパケットを送出するネットワーク接続装置において、機密保護し得ない範囲を送出経路毎に記憶させておく機密保護必要経路記憶部と、暗号化および復号化処理部と、パケットの最終宛先に基づいて選定した転送経路が前記機密保護必要経路記憶部に記憶されている機密保護必要経路を通過するものである場合にパケットのネットワーク層に関するデータの暗号化を決定する暗号化決定部と、機密保護し得ない範囲を抜けたところに位置するネットワーク接続装置を前記暗号化したデータの最終宛先として処理するカプセル化部とを具え、カプセル化したデータをパケットに組み込んで送出することとした。

【0033】また、コネクションレス型パケットを用いて通信する複数のサブネットワークがネットワーク接続装置を介して接続されて成るネットワークにおけるネットワーク通信方式において、送信側のネットワーク接続装置では、受け取ったパケットの最終宛先までの経路中に機密保護し得ない範囲が含まれている場合に、受け取ったパケットのネットワーク層に関するデータを暗号化し、前記範囲を越えた個所にあるネットワーク接続装置を前記暗号化したデータの最終宛先として新たなパケットに組み込んで送出し、最終宛先とされたネットワーク接続装置では、暗号化されたデータを復号化して次へ送出することとした。

【0034】

【作　　用】本発明では、コネクションレス型パケットを用いて通信する複数のサブネットワークがネットワーク接続装置を介して接続されて成るネットワークにおいて、機密保護し得ないサブネットワークを挟んだ地点間

で機密の通信をしようとする場合に、それらの地点に、特別の構成を持ったネットワーク接続装置を設置する。

【００３５】このネットワーク接続装置では、そこから送信する経路中に機密保護し得ない範囲がある場合には、最初の送信終端装置および最後の宛先終端装置のアドレス情報を含めてデータを暗号化し、それを機密保護し得ない範囲を抜けたところに位置するネットワーク接続装置宛のパケット構成にして送る（カプセル化）。それを受け取ったネットワーク接続装置は、暗号化されたデータを復号化し、最終宛先の終端装置へ、通常のパケット構成で送る。

【００３６】機密保護し得ない範囲内にあっては、その範囲を抜けたところに位置するネットワーク接続装置あての通常のパケットという形で通過するから、一体どの終端装置同士の間で通信が行われたのかということを隠すことが出来る。また、データは暗号化されているから、その内容を隠すことが出来る。

【００３７】

【実施例】以下、本発明の実施例を図面に基づいて詳細に説明する。図１は、本発明のネットワーク接続装置である。符号は図２のものに対応し、４０は暗号化・復号化処理部、４１はデータカプセル化部、４２は暗号化決定部、４３は機密保護必要経路記憶部である。これらは、機密保護のために特別に設けられた構成である。このような構成を有するネットワーク接続装置を、機密保護できるサブネットワークと出来ないサブネットワークとの接続部分に設置する。以下、各構成部について説明する。なお、図２と同じ符号のものは同様の動作，機能を果たすので、その説明は省略する。

【００３８】機密保護必要経路記憶部４３は、どの経路でパケットを送る場合は、どのネットワーク接続装置までは機密保護が保証されていないかを記憶しておく。例えば、図１０のネットワーク接続装置７の機密保護必要経路記憶部４３は、サブネットワークＢの方向に送り出す場合、ネットワーク接続装置９までは機密保護が保証されないと記憶しておく。

【００３９】暗号化決定部４２は、経路選択部１１で選択した経路が機密保護必要経路記憶部４３に記憶してある経路に相当するか否かを調べ、相当する場合には、図７のパケットデータ２４Ｄを暗号化することを決定する。暗号化は、暗号化・復号化処理部４０で行う。暗号化の手法は、任意のものを採用することが出来る。暗号化・復号化処理部４０は、暗号化されたデータを受け取った時に、復号化することも行う。

【００４０】データカプセル化部４１は、機密保護し得ない範囲を抜けたところに位置するネットワーク接続装置をあたかも最終宛先とし、自己のネットワーク接続装置をあたかも最初の送信元として、前記の暗号化データを送信データとしてパケット内に組み込む（これを、説明の便宜上、「カプセル化」ということにする）処理をする。

【００４１】図３は、暗号化データをカプセル化したパケットの構成を示す図である。符号は図７のものに対応し、３１はカプセル構成体、３２はプロトコルおよびFixedPart、３３は最終宛先ネットワーク接続装置ネットワークアドレス、３４は送信元ネットワーク接続装置ネットワークアドレス、３５はその他の情報部、３６は暗号化データ格納部である。

【００４２】本発明のネットワーク接続装置で、受け取ったパケットを解析した結果、機密保護が出来ない経路に送り出さなければならないことが判明した時には、ネットワーク層に関するパケットデータ２４Ｄを暗号化し、それを通常のパケットの送信データと同じ扱いとして、暗号化データ格納部３６に格納する。

【００４３】そして、通常のパケット構成では、最終宛先装置ネットワークアドレス２７（図７参照）に相当するところの最終宛先ネットワーク接続装置ネットワークアドレス３３に、機密保護し得ない範囲を抜けたところに位置するネットワーク接続装置のネットワークアドレスを記載する。また、通常のパケット構成では、送信元装置ネットワークアドレス２８（図７参照）に相当するところの送信元ネットワーク接続装置ネットワークアドレス３４に、自己のネットワークアドレス即ちパケットを発送しようとしているネットワーク接続装置のネットワークアドレスを記載する。

【００４４】図４は、カプセル化データを格納したパケットの具体例を示す。これは、図１０のネットワークで、ネットワーク接続装置７，９間は機密保護し得ない範囲であるので、両者間で機密が漏れない通信をするために、ネットワーク接続装置７，９として本発明のネットワーク接続装置を使用しているという環境において、終端装置１から終端装置６へ送るパケットが、ネットワーク接続装置７で作り直された状態のものである。

【００４５】符号は図３のものに対応している。送信元装置ネットワークアドレス２８のアドレスが終端装置１のネットワークアドレス（１Ｎ）とされ、最終宛先装置ネットワークアドレス２７が終端装置６のネットワークアドレス（６Ｎ）とされたパケットデータ２４Ｄが、そのままの形で暗号化され、暗号化データ格納部３６に格納される。送信元ネットワーク接続装置ネットワークアドレス３４は、このパケットを今まさに発送しようとしているネットワーク接続装置７のネットワークアドレス（７Ｎ）とされている。最終宛先ネットワーク接続装置ネットワークアドレス３３は、機密保護し得ない範囲を抜けたところに位置するネットワーク接続装置９のネットワークアドレス（９Ｎ）とされている。

【００４６】送信サブネットワークアドレス２２は、このパケットを今まさに発送しようとしているネットワーク接続装置７の、サブネットワークＢに関するサブネットワークアドレス（７Ｂ）とされ、宛先サブネットワー

クアドレス２１は、当面の送り先であるネットワーク接続装置８の、サブネットワークＢに関するサブネットワークアドレス（８Ｂ）とされている。

【００４７】パケットがこのような構成で送られれば、機密保護し得ない途中のネットワーク接続装置では、最初の送信元がネットワーク接続装置７，最終的な宛先がネットワーク接続装置９である通常のパケットとして取り扱われる。従って、真の送信元や真の最終宛先がどこであるかは全く分からないままで、機密保護し得ない範囲を抜けたところに位置するネットワーク接続装置まで送られて行く。また、仮に途中のネットワーク接続装置で送信データを盗もうとしても、その部分は暗号化されているから、内容を知ることは出来ない。

【００４８】機密保護し得ない範囲を抜けたところに位置するネットワーク接続装置９も、本発明の構成を有するネットワーク接続装置とされているわけであるが、パケットを受け取ると、暗号化されカプセル化されて来たものかどうか判断する。その判断は、送信元がどこであるかということと（上例の場合、ネットワーク接続装置７）、機密保護必要経路記憶部４３に登録されている経路を通って来たかどうかということとを調べて行う。

【００４９】暗号化されたものであることが判明した場合には、暗号化・復号化処理部４０により元のパケットデータ２４Ｄに復号化し、これを通常のパケット構成で、真の最終宛先である終端装置６へ送る。

【００５０】図５は、本発明のネットワーク接続装置の上述したような送信動作を表すフローチャートである。

ステップ１…パケットを受け取る。

ステップ２…受け取ったパケットを解析し、経路を選択し、次に送信する宛先を決定する。

ステップ３…選択した経路が、機密保護の措置をとることが必要な経路かどうかを、機密保護必要経路記憶部４３を参照してチェックする。通らなければ、機密保護の措置をとることなく次へ送信する。

ステップ４…機密保護を必要とする経路を通る場合は、送信データを最終宛先および最初の送信元の情報を含めて暗号化する。

ステップ５…暗号化したデータを、カプセル化する。

ステップ６…次の宛先に送信する。

【００５１】なお、本発明のネットワーク通信方式を実施するには、ネットワーク全体のネットワーク接続装置を本発明の構成のものに変える必要はなく、単に機密保護をした通信をしようとしている地点にのみ、本発明のネットワーク接続装置を設置すればよいので、安いコストで容易に実施することが出来る。

【００５２】

【発明の効果】以上述べた如く、本発明のネットワーク接続装置およびネットワーク通信方式によれば、機密保護し得ないサブネットワークを挟んだ地点間で機密の通信をしようとする場合に、そこから送信する経路中に機密保護し得ない範囲がある場合には、最初の送信終端装置および最後の宛先終端装置を含めてデータを暗号化し、それを機密保護し得ない範囲を抜けたところに位置するネットワーク接続装置宛のパケット構成にして（カプセル化して）送る。

【００５３】そのため、機密保護し得ない範囲内にあっては、その範囲を抜けたところに位置するネットワーク接続装置あての通常のパケットという形で通過するから、一体どの終端装置同士の間で通信が行われたのかということを隠すことが出来る。また、データは暗号化されているから、その内容を隠すことが出来る。

【図面の簡単な説明】

【図１】　本発明のネットワーク接続装置

【図２】　従来のネットワーク接続装置

【図３】　カプセル化データを格納したパケットの一般的な構成を示す図

【図４】　カプセル化データを格納したパケットの具体例を示す図

【図５】　本発明のネットワーク接続装置の送信動作を表すフローチャート

【図６】　Black のサブネットワークとWhite のサブネットワークとが含まれているネットワークの１例を示す図

【図７】　パケットの構成を示す図

【図８】　開放型システム間相互接続の基本参照モデルを示す図

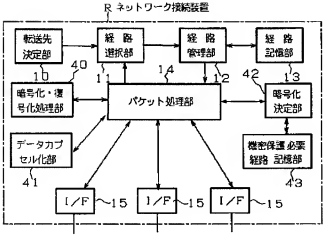
【図９】　図１０のネットワークを搬送されるパケットの構成の変化を示す図

【図１０】　複数のサブネットワークから成るネットワークの他の例を示す図

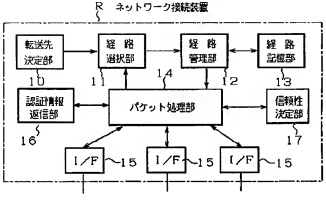
【符号の説明】

１～６…終端装置、７～９…ネットワーク接続装置、１０…転送先決定部、１１…経路選択部、１２…経路管理部、１３…経路記憶部、１４…パケット管理部、１５…インタフェース、１６…認証情報返信部、１７…信頼性決定部、２０…パケット、２４Ｄ，２４D_1，２４D_2…パケットデータ、３１…カプセル化構成体、４０…暗号化・復号化処理部、４１…データカプセル化部、４２…暗号化決定部、４３…機密保護必要経路記憶部、５０～５６…ネットワーク接続装置、５７～５９…終端装置、Ａ～Ｈ，Ｋ…サブネットワーク、Ｒはネットワーク接続装置

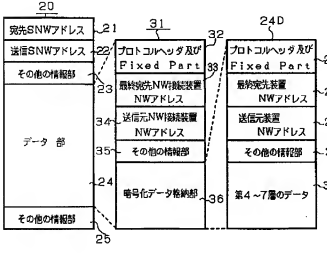
【図１】



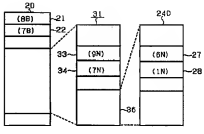
【図２】



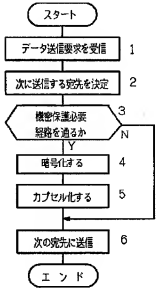
【図３】



【図４】



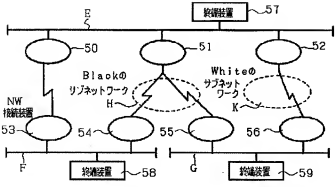
【図５】



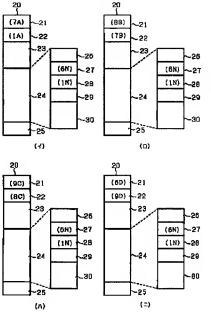
【図８】

局番号	層 名 称
7	アプリケーション
6	プレゼンテーション
5	セッション
4	トランスポート
3	ネットワーク
2	データリンク
1	物 理

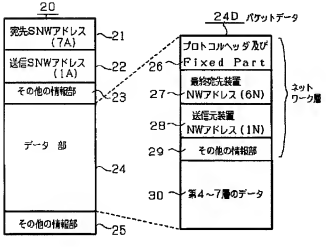
【図６】


E
57
終端装置
50
51
52
Blackの
サブネットワーク
H
Whiteの
サブネットワーク
K
NW
接続装置
53
54
55
56
F
58
終端装置
G
59
終端装置

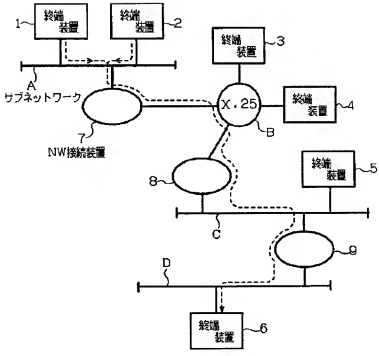
【図９】


20
(7A)
(1A)
21
22
23
(6N)
(1N)
24
25
26
27
28
29
30
(イ)
(BB)
(7B)
(ロ)
(9C)
(8C)
(ハ)
(9D)
(8D)
(ニ)

【図７】


20
24D パケットデータ
宛先SNWアドレス
(7A)
21
送信SNWアドレス
(1A)
22
その他の情報部
23
データ 部
24
その他の情報部
25
プロトコルヘッダ及び
Fixed Part
26
最終宛先装置
NWアドレス (6N)
27
送信元装置
NWアドレス (1N)
28
その他の情報部
29
第4～7層のデータ
30
ネットワーク層

【図１０】



フロントページの続き

(51) Int. Cl.5	識別記号	庁内整理番号	FI		技術表示箇所
Ｈ０４Ｌ 9/12					
12/28					
12/56					
		8529－5K	Ｈ０４Ｌ 11/00	３１０ Ｃ	
		8529－5K	11/20	１０２ Ｄ	